National Security Agency/Central Security Service

INFORMATION
ASSURANCE
DIRECTORATE

CGS Decommission Capability

Version 1.1.1

The Decommission Capability includes the execution of technical and administrative procedures prior to, during, and following removal and disposal of hardware, software, and data assets. During decommission, approved procedures are employed, which maintain information assurance (IA) and prevent the inadvertent compromise of data. This may include sanitization, declassification, and additional releasability procedures.

07/30/2012

CGS Decommission Capability

Version 1.1.1

Table of Contents

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1

2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

The Decommission Capability includes the execution of technical and administrative procedures prior to, during, and following removal and disposal of hardware, software, and data assets. During decommission, approved procedures are employed, which maintain information assurance (IA) and prevent the inadvertent compromise of data. This may include sanitization, declassification, and additional releasability procedures.

3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of “good enough” when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

The Decommission Capability encompasses the decommission phase of the system development lifecycle and involves the disposal or transition of information, hardware, and software from service. Although this Capability covers the decommission phase, disposal and transition of hardware and software assets, including spares, and data assets (e.g., data at rest) are planned in prior phases of the lifecycle.

Relevant procedures shall be created for transition and decommission in earlier phases of the lifecycle, such as development or the acquisition of commercial off-the-shelf (COTS) solutions, and updated and used within the Decommission Capability. Before decommission occurs, transition and decommission plans shall be created by the Program Manager, which includes a phase-out plan and the procedures necessary for decommission. For systems that are to be transitioned from one project to another, the associated transition and decommission plans shall be defined, followed, and updated prior to any update of the system required to support system transition. The Decommission Capability shall employ services from a program management role or office to ensure that all activities and resources are managed according to the program management plan and are able to meet the IA objectives established.

The Enterprise is responsible for defining decommission practices based on policies established by the IA Policies, Procedures, and Standards Capability. The transition and decommission plans shall be aligned with governing decommission policies. Decommission and transition plans shall be based on organizationally approved templates to provide consistency across the Enterprise.

Transition and decommission plans shall be tailored to the target system and information. The procedures followed for decommission will be specific to policies and procedures in place for the type of system being decommissioned. The Enterprise shall update each transition and decommission plan when the system owner changes, when a system is subsumed into a larger system of systems, or when any significant security-relevant change occurs.

Information Systems Security Managers (ISSMs) shall provide guidance to system owners on how to manage systems, which includes decommission. Information System Security Officers (ISSOs) shall interface with System Administrators (SAs) who initiate activities involved with decommission of hardware, software, and data assets. The System Security Engineers (SSEs) shall evaluate the larger architecture and understand interdependencies, connectivity of systems and data, and the effect of decommissioning a system (see Understand Mission Flows and Understand Data Flows Capabilities). The SSEs shall interface with the Program Manager or system owner to share the Enterprise vision regarding interdependencies between existing systems. The Designated Authorization Official (DAO) shall have a role in the decommissioning of all information technology (IT) systems. The DAO shall have input to the risk decisions being made regarding decommission of the system, based on the Risk Analysis Capability. The Organizations and Authorities Capability provides an understanding of the full scope of responsibilities established for the DAO.

Decommissioning of hardware includes components within an overall system, such as hard drives. For decommissioning of specialized hardware (e.g., encryptors or other Communications Security [COMSEC] devices), procedures shall be based on policies that take into account special requirements for classified hardware disposal. Disposal of specialized hardware shall be a part of the overall decommissioning process, such that if decommissioning a system of multiple components and cryptographic devices is a part of the system, it shall be a part of the process. During the useful service life of devices, accountability for devices shall be established in accordance with policy. Decommission leverages the Acquisition Capability to ensure that the vendor is notified and the Enterprise is released from its license agreements. When decommissioning hardware, any maintenance agreements affected shall be updated accordingly.

Decommission of software, hardware, and data assets shall be independent of each other. There may be instances where software needs to be decommissioned even though the hardware remains in operation. When this occurs, the appropriate uninstallation and upgrades shall occur and include reporting of the changes to the Configuration Management Capability so that the software repository can be updated. When decommissioning software, proper procedures shall be defined for license management, such that when software is no longer needed, it is uninstalled and accounted for properly, and licenses are released and removed where necessary.

Disposal of data assets shall be governed by the owner of the information. The Program Manager shall verify disposal with the Enterprise that owns the information, and the system owner shall approve the transition and decommission plan. Data Protection and System Protection shall ensure appropriate protections remain in place after decommission.

The overall system documentation shall be updated or retired depending on the components of the system that is being decommissioned. Retirement shall depend on the Enterprise’s policy for document management, which includes considerations for compliance.

After decommission, appropriate documentation and reporting shall occur to ensure the resources are properly reassigned or removed from the asset database, and responsibility for oversight of systems is properly accounted for and resources redistributed appropriately. Hardware Device Inventory and Software Device Inventory are responsible for knowledge of the Enterprise assets, including spares. As part of decommissioning of spares, the Decommission Capability shall report to the asset database that the spare has a different owner. If the system is being reassigned, the new system owner and other affected stakeholders shall be notified. A notification process shall be defined through policies and procedures.

Sanitization and declassification shall be provided by the Data Protection Capability; however, for decommission, the Enterprise shall consider whether the system will be destroyed or reused. Depending on the result of decommission, the Enterprise shall follow the specific policies and procedures in place for the type of system being decommissioned. Nonserviceable, obsolete, salvaged, or excess equipment shall be reported for disposal in accordance with site regulations. When transporting a system, the Enterprise shall follow appropriate physical and environmental protections (see the Physical and Environmental Protection Capability) using organizationally approved policy.

The transition and decommission plans shall be stored in a centralized repository. The repository shall be associated with the Enterprise's accreditation repository (e.g., where other information is stored regarding system accreditation and risk analysis information). When a change to a transition or decommission plan occurs, automated notification shall be sent to the system owner(s) for the associated accredited system so that updates can occur to the system security plans (SSP) or subsequent security documentation.

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. Physical and environmental protections are defined and implemented.
2. System owners, including owners of hardware, software, and data, are known.
3. The Enterprise has identified systems or components that need to be decommissioned.
4. The Enterprise has defined policies for decommission.
5. All programs have an established program management role or office to manage activities and resources.

5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability follows approved sanitization, declassification, destruction, and clearing procedures, as applicable.
2. All software, hardware, and information will eventually be decommissioned.
3. Approved decommission procedures are defined in accordance with policy.

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

When the Decommission Capability is implemented correctly, the Organization will develop a transition plan and decommission plan prior to transition or disposal of hardware, software, and data assets. Decommission planning is best done as part of the development phase or during the acquisition of COTS solutions, so full resource requirements for transition and disposal are understood and planned for. Throughout the lifecycle, this can be done as hardware and software become obsolete or damaged. In other phases, it will require the tasks outlined in this phase.

Organizations will designate a Program Manager to create transition and decommission plans, which contain the phase-out plan and procedures for decommission. The Program Manager will ensure proper decommission forms exist for activities such as shipping equipment, turning in excess equipment, and transferring accountability for equipment. The Program Manager will also identify system and data ownership and coordinate logistics for the disposal or transfer of a system. Each Program Manager will ensure the system owners provide input to each plan. In some cases, data owner(s) may be different from the system owner, and input will be solicited from both. Organizations will consult with agency Records Management, Privacy, and Freedom of Information Act (FOIA) officials prior to disposal, to ensure compliance with these laws and applicable agency policy. The Organization's transition plans and decommission plans will be stored in a central repository under configuration control, and affected users will be notified of updates.

Organizations will ensure preparation of decommission plans includes coordination and collaboration with multiple roles, including SSEs, to ensure that risk management processes are followed by the Organization. The decommission plan will be defined, understood, vetted, and accepted, leveraging system and security experts, accrediting authorities, and security stakeholders. Organizations will establish the appropriate approval process, which involves an accreditation authority for decommissioning of systems and data assets. If the system has been certified and accredited, prior to decommission, the accreditation authority will be made aware that the system needs to be removed from service.

As part of the Hardware Device Inventory and Software Inventory Capabilities, each Organization will maintain an asset database, which contains the hardware and software inventories. This database will be updated during Decommission Capability activities. During the decommissioning of systems, not only do the operational systems need to be considered but also the spares associated with a project need to be decommissioned as the components of the project are decommissioned. Organizations will employ property accountability requirements when disposing of a system. Once an asset is disposed of, it is no longer accounted for and ownership is reassigned. When possible, Organizations will consider donation of used IT and/or recycling of hazardous material (HAZMAT) parts. Any redistribution of National Security Systems (NSS) IT assets will go through an Organizational review and threat assessment before redistribution occurs. When the above changes occur, ownership and other properties, such as HAZMAT, will be changed in the inventory database.

Specialized hardware and software systems will require additional decommissioning activities. Organizations will define their procedures for decommissioning of specialized hardware and software systems, which will take into account multiple components and cryptographic devices. For encryptors and COMSEC devices, either the Program Manager or the site shall contact the appropriate authority who will initiate a request to decommission any cryptographic device.

Organizations will ensure acquisition points of contact (POCs) are notified of disposal or removal of devices and ensure devices are removed from vendor support contracts. This is done before or in conjunction with decommissioning an asset. In some cases, an Organization will need to inform the vendor that the asset is being returned/decommissioned. In addition, each Organization will define procedures removing software that is no longer needed. Organizations will ensure licenses are tracked and accounted for when software is removed.

Each Organization will ensure appropriate Data Protection mechanisms are in place for sanitization and declassification. The Organization will consider whether the system will be destroyed or reused, based on Organizational policy/procedures for the specific type of system.

Organizations will coordinate logistics for equipment transfers and disposal. For cost savings, some Organizations may maintain functional but old parts for contingency operations. For example, an Organization will use retired laptops for a telecommuting

scenario that requires only partial processing for vital Internet or email communications once the laptops have been properly sanitized.
As part of the Decommission Capability, information will be moved to another system, archived, discarded, or destroyed. When archiving information, each Organization will consider the method for retrieving the information in the future. For example, although electronic information is generally easier to retrieve and store, the technology used to create the records will not be readily available in the future. Measures will also be taken for the future use of data that has been encrypted, such as taking appropriate steps to ensure the secure long-term storage of cryptographic keys (see the Key Management Capability).

Organizations will ensure documentation and reporting occurs for reassigned or removed systems or data assets, and new system owners will be notified based on the Organization's policy. Organizations will update or retire system documentation based on the system components that are being decommissioned. It is important to consider legal requirements for records retention when disposing of systems or data assets. For federal systems, system management officials within the Organization will consult with their agency office responsible for retaining and archiving federal records.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Network Mapping–The Decommission Capability relies on the Network Mapping Capability to provide information about the current state of the network, which will be factored into decommission decisions made throughout the lifecycle.
- Understand Mission Flows–The Decommission Capability relies on the Understand Mission Flows Capability to provide an understanding of mission context and meaning for mission function component parts to assist with defining the transition and decommission plan.

- Understand Data Flows–The Decommission Capability relies on the Understand Data Flows Capability to provide an understanding of the interdependencies and connectivity of systems and data to assist with defining the transition and decommission plan.
- Configuration Management–The Decommission Capability relies on the Configuration Management Capability to track the changes that occur during system decommission.
- Risk Analysis–The Decommission Capability relies on information from the Risk Analysis Capability to make risk decisions, based on policy, on the type of procedures to follow during decommission.
- Finance–The Decommission Capability relies on the Finance Capability to provide funding, including certification and accreditation funding, throughout decommission.
- Acquisition–The Decommission Capability relies on the Acquisition Capability to ensure that any vendors are notified of decommission activities, as necessary, and the Enterprise is released from its license agreements.
- Development–The Decommission Capability relies on the Development Capability to plan for the transition and decommission of systems during the development phase.
- Operations and Maintenance–The Decommission Capability relies on the Operations and Maintenance Capability to ensure that systems are ready for decommission.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management–The Decommission Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards–The Decommission Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness–The Decommission Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.

- IA Training–The Decommission Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Decommission Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Utilization and Performance Management–The Decommission Capability relies on the Utilization and Performance Management Capability to provide information about components that cause degraded performance or do not meet targets or service level agreements (SLAs). This information aids the decision-making process on whether to decommission a device or component.
- System Protection–The Decommission Capability relies on the System Protection Capability to provide protection mechanisms for systems that have been decommissioned.
- Physical and Environmental Protections–The Decommission Capability relies on the Physical and Environmental Protections Capability to provide physical and environmental protections when decommission is performed onsite, as well as when transporting a system from the original site to the decommission site.
- Data Protection–The Decommission Capability relies on the Data Protection Capability to ensure that data is protected during and after a system is decommissioned.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	
MP-6 *MEDIA SANITIZATION*	Control: The organization sanitizes information system media, both digital and non-digital, prior to disposal, release out of

	organizational control, or release for reuse. Enhancement/s: (1) The organization tracks, documents, and verifies media sanitization and disposal actions. (2) The organization tests sanitization equipment and procedures to verify correct performance [Assignment: organization-defined frequency]. (3) The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: [Assignment: organization-defined list of circumstances requiring sanitization of portable, removable storage devices]. (4) The organization sanitizes information system media containing Controlled Unclassified Information (CUI) or other sensitive information in accordance with applicable organizational and/or federal standards and policies. (5) The organization sanitizes information system media containing classified information in accordance with NSA standards and policies. (6) The organization destroys information system media that cannot be sanitized.
SI-13 *PREDICTABLE FAILURE PREVENTION*	Control: The organization: a. Protects the information system from harm by considering mean time to failure for [Assignment: organization-defined list of information system components] in specific environments of operation; and b. Provides substitute information system components, when needed, and a mechanism to exchange active and standby roles of the components. Enhancement/s: (1) The organization takes the information system component out of service by transferring component responsibilities to a substitute component no later than [Assignment: organization-defined fraction or percentage] of mean time to failure.

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Decommission Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoDD 5000.01, The Defense Acquisition System, 20 November 2007, Unclassified	Summary: Consistent with statute and the regulatory requirements specified in this directive and in Department of Defense Instruction (DoDI) 5000.02, every Program Manager (PM) shall establish program goals for the minimum number of cost, schedule, and performance parameters that describe the program over its entire lifecycle. PMs shall consider supportability, lifecycle costs, performance, and schedule comparable in making program decisions. Planning for operation and support and the estimation of total ownership costs shall begin as early as possible. Supportability, a key component of performance, shall be considered throughout the system lifecycle.
DoDI 5000.02, Operation of the Defense Acquisition System, 8 December 2008, Unclassified	Summary: This instruction implements Department of Defense Directive (DoDD) 5000.01 by establishing a simplified and flexible management framework for translating capability needs and technology opportunities, based on approved capability needs, into stable, affordable, and well-

	managed acquisition programs that include weapon systems, services, and automated information systems. It describes the five phases of the Defense Acquisition Management System: Materiel Solution Analysis, Technology Development, Engineering and Manufacturing Development, Production and Deployment, and Operations and Support [through decommission]. Systems engineering shall be embedded in program planning and be designed to support the entire acquisition lifecycle.
DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007, Unclassified	Summary: This instruction establishes the DoD Information Assurance Certification and Accreditation Process (DIACAP) for authorizing the operation of DoD information systems. The process manages the implementation of information assurance (IA) capabilities and services and provides visibility of accreditation decisions. The DIACAP requirements, activities, and tasks described are applicable throughout the information system's lifecycle, which includes decommission.
DoDI 8580.1, Information Assurance (IA) in the Defense Acquisition System, 9 July 2007, Unclassified	Summary: IA shall be implemented in all system and services acquisitions at levels appropriate to the system characteristics and requirements throughout the entire lifecycle of the acquisition in accordance with an adequate and appropriate Acquisition IA Strategy that shall be reviewed prior to all acquisition milestone decisions, program decision reviews, and acquisition contract awards.
Defense Acquisition Guidebook, https://dag.dau.mil/Pages/Default.aspx, 17 December 2009, Unclassified	Summary: This guidebook complements DoDD 5000.01 and DoDI 5000.02 by providing the acquisition workforce with discretionary best practices that should be tailored to the needs of each program. Section 4.3, Systems Engineering in the System Life Cycle, provides an integrated technical framework for systems engineering activities throughout the acquisition phases of a system's lifecycle, highlighting the particular systems engineering inputs, activities, products, technical reviews, and outputs of each acquisition phase.
Committee for National Security Systems (CNSS)	
Nothing found	

Other Federal (OMB, NIST, …)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	

Decommission Standards

Title, Date, Status	**Excerpt / Summary**
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
NIST SP-800-64 Rev 2, Security Considerations in the System Development Life Cycle, October 2008, Unclassified	Summary: This special publication focuses on the information security components of the system development lifecycle (SDLC). It describes the key security roles and responsibilities that are needed in development of most information systems. Its scope is security activities that occur within the linear, sequential (a.k.a. waterfall) SDLC methodology. The five-step SDLC cited in this document (includes Decommission [as Disposal]) is an example of one method of development and is not intended to mandate this methodology.

Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, …)	
ISO/IEC 15288:2008, Systems and Software Engineering–System Life Cycle Processes, 1 February 2008, Unclassified	Summary: This document provides a common process framework and the processes for acquiring and supplying systems. These processes can be applied at any level in the hierarchy of a system's structure. Selected sets of these processes can be applied throughout the full system lifecycle (e.g., conception of ideas, development, production, utilization, support, and retirement of the system) and to the acquisition and supply of systems.
IEEE 1220-2005, IEEE Standard for Application and Management of the Systems Engineering Process, 9 September 2005, Unclassified	Summary: This standard defines the interdisciplinary tasks that are required throughout a system's lifecycle to transform stakeholder needs, requirements, and constraints into a system solution. It is intended to guide the development of systems for commercial, government, military, and space applications and applies to projects within an Enterprise that is responsible for developing a product design and establishing the lifecycle infrastructure needed for lifecycle sustainment.
International Council on Systems Engineering (INCOSE) Systems Engineering Handbook, version 3.1, 2007, Unclassified	Summary: This handbook describes the key process activities performed by systems engineers, covering in detail the purpose for each process activity, what needs to be done, and how to do it. It provides sufficient information to determine whether a given process activity is appropriate in supporting program objectives and how to go about implementing the process activity.

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Recycling–As part of decommissioning, if the Organization allows for recycling parts, it can recoup some of its costs.
2. Complexity of systems being decommissioned–More complex systems may require more resources and time to decommission.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Decommission Capability.

- The Enterprise shall be responsible for the disposal or transition of information, hardware, software, and data assets from service.
- The Enterprise shall create relevant procedures for transition and decommission in earlier phases of the lifecycle, such as development or the acquisition of COTS solutions.
- The Program Manager shall create a phase-out plan and procedures before transition and decommission occurs.
- For systems that are to be transitioned from one project to another, the associated transition and decommission plans shall be defined, followed, and updated prior to any update of the system required to support system transition.
- The Enterprise shall employ services from a program management role or office to ensure that all activities and resources are managed according to the program management plan and are able to meet the IA objectives established.

- The Enterprise shall define decommission practices based on policies established by the Enterprise's policies, procedures, and standards.
- The transition and decommission plans shall be aligned with governing decommission policies.
- Decommission and transition plans shall be based on organizationally approved templates to provide consistency across the Enterprise.
- Transition and decommission plans shall be tailored to the target system and information.
- The Enterprise shall update each transition and decommission plan when the system owner changes, when a system is subsumed into a larger system of systems, or when any significant security-relevant change occurs.
- ISSMs shall provide guidance to system owners on how to manage systems, which includes decommission.
- ISSOs shall interface with system administrators who initiate activities involved with decommission of hardware, software, and data assets.
- The SSEs shall evaluate the larger architecture and understand interdependencies, connectivity of systems and data, and the effect of decommissioning a system.
- The DAO shall have a role in the decommissioning of all IT systems.
- The DAO shall have input to the risk decisions being made regarding decommission of the system, based on the risk analysis.
- For decommissioning of specialized hardware (e.g., encryptors or other COMSEC devices), the Enterprise shall have procedures based on policies that take into account special requirements for classified hardware disposal.
- Disposal of specialized hardware shall be a part of the overall decommissioning process, such that if a system of multiple components and cryptographic devices is a part of the system, it shall be a part of the process.
- During the useful service life of devices, accountability for devices shall be established in accordance with policy.
- When hardware is being decommissioned, any maintenance agreements affected shall be updated accordingly.
- Decommission of software, hardware, and data assets shall be independent of each other.
- All uninstallation and upgrades shall occur and include reporting of the changes to the configuration management so the software repository can be updated.
- When software is being decommissioned, proper procedures shall be defined for license management, such that when software is no longer needed, it is

uninstalled and accounted for properly, and licenses are released and removed, where necessary.

- Disposal of data assets shall be governed by the owner of the information.
- The Program Manager shall verify disposal of data assets with the Enterprise that owns the information.
- The system owner shall approve the transition and decommission plan for the disposal of data assets.
- Data Protection and System Protection capabilities shall ensure appropriate protections remain in place after decommission.
- The overall system documentation shall be updated or retired depending on the components of the system that is being decommissioned.
- Retirement shall depend on the Enterprise's policy for document management, which includes considerations for compliance.
- After decommission, appropriate documentation and reporting shall occur to ensure the resources are properly reassigned or removed from the asset database, and responsibility for oversight of systems is properly accounted for and resources redistributed appropriately.
- As part of decommissioning of spares, the Enterprise shall report to the asset database that the spare has a different owner.
- A notification process shall be defined through policies and procedures.
- The Enterprise shall consider whether the system will be destroyed or reused.
- The Enterprise shall follow the specific policies and procedures in place for the type of system being decommissioned.
- Nonserviceable, obsolete, salvaged, or excess equipment shall be reported for disposal in accordance with site regulations.
- When transporting a system, the Enterprise shall follow appropriate physical and environmental protections when using organizationally approved policy.
- The transition and decommission plans shall be stored in a centralized repository.
- The repository shall be associated with the Enterprise's accreditation repository (e.g., where other information is stored regarding system accreditation and risk analysis information).
- For all changes to a transition or decommission plan that occur, an automated notification shall be sent to the system owner(s) for the associated accredited system so that updates can occur to the SSPs or subsequent security documentation.